

Application No.: 10/073,261

Docket No.: 1509-275

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A storage device, comprising: including

a trusted clock,

a memory,

a time-stamper,

an interface,

a controller, and

a digital signer,

wherein

the controller is configured device being adapted in use to cause store to said memory data, that has been received from an outside of said device via said interface, to be time-stamped by said time-stamper, with a time obtained from said trusted clock, and digitally signed with a digital signature by said digital signer, and

the controller is further configured to store the time-stamped and digitally signed data to said memory, without transmitting said time-stamped data back to the outside of said device.

2. (currently amended) A device as claimed in claim 1, wherein said memory comprises either of the following at least one selected from the group consisting of: a disc, and a tape drive.

3. (currently amended) A device as claimed in claim 1, wherein said memory is a long term storage medium.

Application No.: 10/073,261

Docket No.: 1509-275

4. (currently amended) A device as claimed in claim 1, wherein said memory is a removable ~~from the storage device~~ storage medium.
5. (currently amended) A device as claimed in claim 1, wherein said device comprises a part of ~~any one of the following~~ one selected from the group consisting of: a disc drive, a tape drive, a disc array, a disc sub-system, a tape library, an optical jukebox, a disaggregated storage network, a storage area network, network attached storage.
6. (currently amended) A device as claimed in claim 1, wherein said trusted clock is provided by a replaceable card pluggable ~~adapted to be plugged~~ into said device.
7. (currently amended) A device as claimed in claim 1, wherein said trusted clock is an encapsulated hardwired component.
8. (currently amended) A device as claimed in claim 1, further comprising ~~wherein there is a controller, with associated~~ controller logic associated with said controller, said controller logic being protected by a trusted mechanism to prevent unauthorized ~~unauthorized and unnoticed~~ alteration of said controller logic.
9. (currently amended) A device as claimed in claim 1, wherein said ~~device has a~~ controller is further configured ~~adapted~~ to do at least one of the following:
- (i) identify whether the data received via said interface ~~by said device~~ has a flag indicative as a command to time-stamp the flagged data,
 - (ii) identify whether command language used to control operation of said device has a marker indicative as a command to time-stamp selected data, and
 - (iii) check whether the time-stamper is set to a time-stamp mode to time-stamp received data, or ~~not, so set so as not to time-stamp data~~ not.

Application No.: 10/073,261

Docket No.: 1509-275

~~10.~~ (currently amended) A device as claimed in claim 1, further comprising a clock-correcting input adapted to input a trusted correction signal to said trusted clock to correct said clock.

~~11.~~ (canceled)

~~12.~~ (currently amended) A storage device as claimed in claim 8, wherein said memory is including a trusted clock; a long term memory device; a time stamper; a digital signing unit; and a controller, with associated controller logic; said device being adapted, in use, to store to said memory device data that has been time stamped by said time stamper with a time obtained from said trusted clock and digitally signed with a digital signature by said digital signing unit; and said controller logic being protected by a trusted mechanism to prevent, in use, unauthorized alteration of said controller logic.

~~13.~~ (currently amended) A storage device, comprising: including
trusted clock means for non-repudiably measuring time,
~~data storage means for storing data;~~
time-stamping means for stamping data with a non-repudiable time supplied by said trusted clock means,
digital signing means for signing data digitally,
~~such that said data storage means for locally storing stores~~ data that has been time-stamped by said time-stamping means and signed with a digital signature by said digital signing means,
[[in use]] and
controlling means for prohibiting transmission of said time-stamped data to components other than said digital signing means and said data storage means.

Application No.: 10/073,261

Docket No.: 1509-275

14. (previously presented) A method of storing secure time-stamped data in a data storage device, a trusted clock being at the data storage device, comprising the steps of:

- (i) time-stamping data by using the trusted clock at said data storage device;
- (ii) creating a digital signature dependent upon content of said data and time-stamp; and
- (iii) storing said data and the signature associated with said data in said data storage device on a recording medium of said data storage device.

15. (currently amended) A method as claimed in claim 14, wherein said recording medium where said data storage device comprises a long-term data storage medium, and wherein time-stamped, signed data are stored on said long-term data storage medium.

16. (currently amended) A method as claimed in claim 14, wherein said data storage device comprises a controller ~~[[is]]~~ used to control ~~operations~~ steps (i) to (iii), ~~and wherein~~
said controller is controlled by control logic, and
said method further comprises protecting said control logic by a trusted mechanism which ensures that said control logic has not been modified from what it should be to prevent unauthorized alteration of said controller logic.

17. (currently amended) A method as claimed in claim 14, further comprising including checking data received by said data storage device for a flag indicative of instructions to time-stamp all of or a selected part of said data, and said data, or the part of said data, is time stamped accordingly.

18. (currently amended) A method as claimed in claim 14, further comprising including checking a command language of a controller in said data storage device, said

Application No.: 10/073,261

Docket No.: 1509-275

controller being used to control steps (i) to (iii), for instructions to time-stamp all, or a selected part, or parts, of said data.

19. (currently amended) A method as claimed in claim 14, wherein
said device comprises is controlled by a controller which is used to control steps (i) to (iii) and
which has a time-stamp setting in which the time-stamper time-stamps said data and a non
time-stamping setting in which the time-stamper does not time-stamp said data, and
said method further comprises checking in which a check is made as to the setting of said
controller prior to said operation (i) time-stamping, or not, of received said data.

20. (currently amended) A method of storing secure time-stamped data in a data storage
device, a trusted clock being at the data storage device, said method comprising the steps of:
transmitting data to said device over the Internet or other public network;
time-stamping said data by using the trusted clock at said data storage device;
creating a digital signature dependent upon content of said data and time-stamp; and
storing said data and the signature associated with said data on a recording medium of said data
storage device, as claimed in claim 14 comprising transmitting said data to said device over the
Internet or other public network, and time-stamping and signing said data, and storing said
time-stamped signed data, within said data storage device without transmitting said signed
time-stamped data back over the Internet or other public network.

21. (currently amended) A method as claimed in claim 14, wherein said data that is time-stamped is a digest of a larger data record.

22. (canceled)

Application No.: 10/073,261

Docket No.: 1509-275

~~23.~~ (currently amended) A network, comprising having a data storage device adapted to time-stamp and store data that [[it]] said data storage device receives from said network without transmitting time-stamped data across said network.

~~24.~~ (currently amended) ~~A Software, firmware or a computer readable medium~~ comprising having a program recorded thereupon, said program when executed by which, in use, causes a processor of a data storage device running a program causes the processor to execute a process including:

- i) time-stamping data by using a trusted clock at said data storage device;
- ii) creating a digital signature dependent upon content of said data and time-stamp; and
- iii) storing said data and associated said signature on a recording medium of said data storage device without transmitting said time-stamped data outside said data storage device.

~~25.~~ (canceled)

~~26.~~ (currently amended) A method of storing time-stamped ~~time-stamper~~ data on a network, said method comprising:

transmitting [[the]] data from a data source connected to said network ~~first, remote, network-attached device~~ to a data storage device also connected to said network, the data storage device including a trusted clock, a memory, a time-stamper and a digital signer,

time-stamping and digitally signing the transmitted data at said data storage device using ~~storing in said memory data that have been time-stamped by said time-stamper, the stored data including a time obtained from said trusted clock and digitally signed with a digital signature by said digital signer, and~~

storing the time-stamped and digitally signed data to said memory, without in the absence of transmitting time-stamped data back to said ~~remote device for storage~~ data source via said network.

Application No.: 10/073,261Docket No.: 1509-275

27. (new) A device as claimed in claim 8, wherein said controller logic is time-stamped.
28. (new) A method as claimed in claim 14, wherein
said data storage device comprises a controller used to control steps (i) to (iii),
said controller is controlled by control logic, and
said method further comprises time-stamping the controller logic prior to passing data through
to the trusted clock.
29. (new) A method as claimed in claim 14, wherein
said data storage device comprises a controller used to control steps (i) to (iii),
said controller is controlled by control logic, and
said method further comprises checking a signature of the controller logic prior to step (i).

726/20
Data
authentication